

SDD:SK  
F. #2017R01829

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

18M187

-----X

UNITED STATES OF AMERICA

COMPLAINT

- against -

(18 U.S.C. § 1349)

JOSHUA PHILIPS,  
also known as "Erick Ayo Kalu,"  
"Anthony Abongile Baker," and  
"Johnson Foday Brown," and  
[REDACTED]

Defendants.

-----X

EASTERN DISTRICT OF NEW YORK, SS:

PAUL BERNARDI, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between June 2017 and December 2017, within the Eastern District of New York and elsewhere, the defendants JOSHUA PHILIPS, also known as "Erick Ayo Kalu," "Anthony Abongile Baker," and "Johnson Foday Brown," and [REDACTED] together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud individuals and businesses, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings,

signs, signals, pictures and sounds, to wit: remote access of computers in the United States and elsewhere, wire transfers, telephone calls and emails, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2015. I have been involved in the investigation of numerous cases involving cybercrime, financial fraud and money laundering, during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in the investigation; (b) my review of the investigative file; and (c) reports made to me by witnesses and other law enforcement officers involved in the investigation.

---

<sup>1</sup> Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

### Business Email Compromise and Confidence Fraud

3. Business email compromise is a form of cyber-enabled financial fraud. In a typical business email compromise scheme, a malicious actor compromises legitimate business email accounts through computer intrusion techniques or social engineering and uses those accounts to cause the unauthorized transfer of funds. Cybercrime techniques for perpetrating these schemes include spear phishing,<sup>2</sup> identity theft, spoofing of emails and websites, and the use of malware.

4. Confidence fraud is another form of cyber-enabled financial fraud. In a typical confidence fraud, a malicious actor befriends, and gains the confidence of, another individual through online communications and uses that confidence to cause the transfer of funds for unauthorized purposes.

### The Compromise of Individuals in the Eastern District of New York

5. Since approximately October 2017, the FBI has been conducting an investigation into a business email compromise scheme in which the defendants and others targeted individuals and businesses in the Eastern District of New York and elsewhere. The targeted individuals included an individual in Long Island, New York ("John Doe 1"), and his real estate attorney in Long Island, New York ("John Doe 2").

6. In or about and between July 2017 and August 2017, John Doe 1 engaged in a real estate transaction involving the purchase of property in Massapequa, New York. John Doe 2 served as John Doe 1's real estate attorney for the transaction and facilitated the purchase.

---

<sup>2</sup> Spear phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

7. John Doe 1 and John Doe 2 communicated by email regarding the transaction. For example, on or about August 18, 2017, John Doe 2 forwarded John Doe 1 an email regarding the scheduling of a closing date with the relevant counterparties to the transaction. That same day, John Doe 1 responded to the email, stating, among other things, "Thanks [John Doe 2] I know your [sic] on top of it. Just let us know and we will be there."

8. In or about and between August 23, 2017 and August 25, 2017, John Doe 1 received a series of emails from the email account of John Doe 2 asking about the status of the closing funds. For example, on or about August 23, 2017, John Doe 1 received an email from the email account of John Doe 2 asking, "With regards to the closing funds, is it currently available?" After responding affirmatively, John Doe 1 received an email the next day, on or about August 24, 2017, from the email account of John Doe 2 instructing John Doe 1 "to go to your local branch within the day and initiate a wire transfer of the funds to my attorney escrow account indicated below." The August 24, 2017 email then provided bank account information for an account at Fifth Third Bank in the name of "Stones Atlanta" (the "Fraud Account").

9. John Doe 2 has informed law enforcement officers, in sum and substance and in part, that he did not send the August 24, 2017 email and that the bank account details contained in the email do not pertain to any account within his control.

10. Records obtained from the online email service provider that hosts the email account of John Doe 2 revealed an aberrant login, on or about August 23, 2017, from a computer associated with an IP address in Africa. John Doe 2 was not responsible for the login.

11. On or about August 28, 2017, John Doe 1 sent a wire transfer in the amount of \$84,000 to the Fraud Account and sent an email confirming the wire transfer to the email account of John Doe 2.

12. Records obtained from Fifth Third Bank revealed that defendant [REDACTED], listed as [REDACTED] with an address in [REDACTED] was the sole signatory of the Fraud Account. A search of law enforcement databases revealed a driver's license issued to defendant [REDACTED] [REDACTED] with the same address in [REDACTED] and a photograph.

13. Records obtained from Fifth Third Bank revealed that, over the course of the next month, [REDACTED] withdrew nearly all of the \$84,000 in funds from the Fraud Account through wire transfers, cashiers' checks, and a series of cash withdrawals. Fifth Third Bank provided the FBI with excerpts of video camera footage related to two of the cash withdrawals. I have reviewed the video camera footage excerpts provided by Fifth Third Bank and have confirmed that the individual making the cash withdrawals is defendant [REDACTED]



The Broader Fraudulent Scheme Compromising Individuals Across the United States

14. The defendant [REDACTED] shared his proceeds with the defendant JOSHUA PHILIPS, also known as "Erick Ayo Kalu," "Anthony Abongile Baker," and "Johnson Foday Brown."

15. Specifically, out of the \$84,000 in funds that [REDACTED] received from the above-described business email compromise scheme, [REDACTED] sent \$35,400 by wire transfer, on or about August 30, 2017, to an account at SunTrust Bank in the name of "Erick Ayo Kalu" ("Personal Account 1"). Personal Account 1 was associated with an address in Lawrenceville, Georgia.

16. Records obtained from SunTrust Bank revealed a separate account in the name of "Erick and Brothers Investments Inc." ("Corporate Account 1") with "Erick Ayo Kalu" as the sole signatory and with the same address in Lawrenceville, Georgia, as Personal Account 1. Records obtained from Chase Bank revealed an account in the name of "JB and Company Inc." ("Corporate Account 2") with "Johnson Foday Brown" as the sole signatory and with an address in Austell, Georgia. Records obtained from Chase Bank revealed an account in the name of "A Baker and Group Investments Inc." ("Corporate Account 3," collectively the "Corporate Accounts") with "Anthony Abongile Baker" as the sole signatory and with an address in Marietta, Georgia. Further investigation revealed that each of the foregoing signatories was an alias for defendant JOSHUA PHILIPS.

17. Records obtained from SunTrust Bank associated with Corporate Account 1 list an email associated with the account as mrrerick83@mail.com (the "Kalu Email"). Records obtained from the online email service provider Mail.com revealed multiple successful logins into the Kalu Email from the IP address 71.204.56.61 (the "Kalu

IP”) in November and December 2017. Records obtained from Comcast revealed that the Kalu IP is associated with the subscriber “JOSHUA PHILIPS” with an address in Ellenwood, Georgia. A search of law enforcement databases revealed a driver’s license issued to defendant JOSHUA PHILIPS, in the name “JOSHUA C PHILIPS” with a different address in Ellenwood, Georgia, and a photograph. Records obtained from First Citizens Bank revealed an account in the name of “Erick Ayo Kalu” involving various cash withdrawals. First Citizens Bank provided the FBI with excerpts of video camera footage related to one of the cash withdrawals. I have reviewed the video camera footage excerpts provided by First Citizens Bank and have confirmed that the individual making the cash withdrawal is defendant JOSHUA PHILIPS. Records obtained from Chase Bank revealed an account in the name of “Joshua Philips” (“Personal Account 2”) involving various cash withdrawals. Chase Bank provided the FBI with excerpts of video camera footage related to one of the cash withdrawals from Personal Account 2, one of the cash withdrawals from Corporate Account 2, and one of the cash withdrawals from Corporate Account 3. I have reviewed the video camera footage excerpts provided by Chase Bank and have confirmed that the individual making the cash withdrawals is defendant JOSHUA PHILIPS. I have also reviewed the identification documents used to open Corporate Account 2 and have confirmed that the individual depicted in each of these documents is defendant JOSHUA PHILIPS.

18. After [REDACTED] sent PHILIPS \$35,400, over the course of the next week, PHILIPS withdrew nearly all of the \$35,400 in funds from Personal Account 1 through wire transfers, cash withdrawals, and personal expenses. On or about August 31, 2017, PHILIPS sent \$20,050 of the funds by wire transfer to an overseas bank account.

19. PHILIPS was also involved in other cyber-enabled fraudulent schemes.

On or about the following dates, an individual in Granada, Minnesota ("John Doe 3") sent the following funds to the Corporate Accounts.

Date	Amount	Account
July 26, 2017	\$17,240	2
August 11, 2017	\$140,000	1
August 24, 2017	\$144,300	1
September 6, 2017	\$78,350	1
December 6, 2017	\$65,000	3
December 26, 2017	\$80,000	3

20. John Doe 3 has informed law enforcement officers, in sum and substance and in part, that: he met a female persona online and communicated with her via email; the female persona asked John Doe 3 to help her obtain her inheritance from a foreign country by paying various fees associated with transferring the money from the foreign country to the United States; John Doe 3 made multiple wire transfers totaling more than \$345,000 to the Corporate Accounts for that purpose; John Doe 3 did not personally know "Erick Ayo Kalu" or "Johnson Foday Brown."

21. After each of John Doe 3's wire transfers to the Corporate Accounts, PHILIPS withdrew nearly all of the transferred funds from the Corporate Accounts through wire transfers, personal and cashiers' checks, and cash withdrawals. PHILIPS made several of the personal checks out to [REDACTED]: from Corporate Account 1 totaling more than



\$16,000 in August 2017; from Corporate Account 2 totaling more than \$10,000 in July 2017; and from Corporate Account 3 totaling more than \$2,000 in December 2017.

22. PHILIPS made one of the cashier's checks, in the amount of \$12,000, out to Copart, Inc. for the benefit of account number 343391. Copart, Inc. is an online vehicle auction company headquartered in Dallas, Texas. Records obtained from Copart, Inc. revealed that account number 343391 belongs to Unijankers Nigeria Limited, an import/export company incorporated in Nigeria that purchased multiple used vehicles with those funds.

23. On or about the following dates, an individual in Pittsburgh, Pennsylvania ("Jane Doe 1") sent the following funds to Corporate Account 2.

Date	Amount
June 16, 2017	\$105,000
July 3, 2017	\$93,000
July 7, 2017	\$57,000

24. Jane Doe 1 has informed law enforcement officers, in sum and substance and in part, that: she met a male persona online and communicated with him via email; the male persona asked Jane Doe 1 to help him leave his company by paying various fees associated with divesting his money; Jane Doe 1 made multiple wire transfers to Corporate Account 2 for that purpose; Jane Doe 1 did not personally know "Johnson Foday Brown."

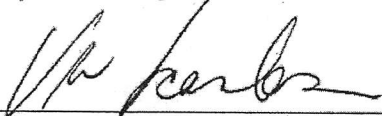
25. After each of Jane Doe 1's wire transfers to Corporate Account 2, PHILIPS withdrew nearly all of the transferred funds from Corporate Account 2 through wire transfers, personal and cashiers' checks, and cash withdrawals.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendants JOSHUA PHILIPS, also known as "Erick Ayo Kalu," "Anthony Abongile Baker," and "Johnson Foday Brown," and [REDACTED], so that they be dealt with according to law. I further request that this affidavit and the arrest warrant be filed under seal as these documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation, and disclosure of these documents would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates, and flee from or evade prosecution.



PAUL BERNARDI  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
2nd day of March, 2018



THE HONORABLE VERA M. SCANLON  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK